Science & Technology Development Journal – Engineering and Technology 2024, 6(SI8):54-60

Open Access Full Text Article

Research Article

Developing a data security solution for the command and control management system at the headquarters

Tran Viet Dung, Nguyen Truc Quyen, Cu Hoai Nam*

ABSTRACT

The construction of an integrated information system to support command and control to meet the requirements of national defense in wartime and peacetime is extremely urgent. In order for this system to be effectively applicable, it is necessary to ensure both the necessary and sufficient conditions. The primary necessary condition is the system's applicability, while the sufficient condition encompasses the complementary measures and solutions within the system to ensure its integrity, authenticity, and robustness. The system is deployed in the Command Post's private network environment, this is the network layer that needs protection and is not connected to the internet. The network system is divided into two parts: secret network and clear network. The secret network contains data of the entire system, so it is necessary to control all connections to this secret network. The clear network can connect to external networks through system information security control devices. To fulfill the system requirements, a comprehensive approach is essential, involving both engineering and personnel aspects. However, within the scope of this article, the authors primarily present a set of hardware solutions aimed at addressing the issue of information protection. This article identifies groups of information that require protection, mitigates security threats, and highlights the existing hardware tools that are suitable for the established operating management system model. The goal of the solution is to ensure absolute information security of the system when deployed in military units. By using experimental methods, analyzing and summarizing experience during the installation and testing process in the laboratory and in practice at the deploying unit, we have achieved the effectiveness of ensuring information security. according to military requirements. However, using this solution will increase the delay in information exchange between devices.

Key words: operating management system, information protection, hardware security solutions

Institute of Information Technology, AMST, Ho Chi Minh City, Vietnam

Correspondence

Cu Hoai Nam, Institute of Information Technology, AMST, Ho Chi Minh City, Vietnam

Email: cuhoainam1234@gmail.com

History

- Received: 20-9-2023
- Accepted: 27-3-2024
- Published Online: 31-12-2024

DOI : 10.32508/stdjet.v6iSI8.1204

INTRODUCTION

The emergence and strong development of science and technology, especially the 4.0 technological revolution, have significantly changed the theoretical and practical aspects of military affairs and altered the methods of conducting warfare, the dimensions of space and time in combat, and even the boundaries of offense and defense. The general trend worldwide is to build efficient and streamlined armed forces, and the automation of command is an inevitable historical necessity to address the contradiction between the increasing volume of various types of information reaching the advisory and command agencies, which becomes larger, more complex, and more frequent, and the demand of modern warfare for information to be processed in the shortest possible time, in real-time.

In parallel with this trend, within the country, various systems serving the management and operation of Command Posts have been researched and equipped, such as the combat command support system, the online briefing system, the security surveillance camera system. However, these systems operate independently and need to be integrated into a coherent system, lacking the ability to transmit combat information in the form of images and videos and not allowing direct connections to seek guidance from leadership.

Therefore, there is a need to integrate these independent information systems into a unified integrated system that has the capability to connect and share data to serve the processing of defense scenarios at the Command Post in order to successfully accomplish national security tasks [1]. However, the issue of security and information protection in this integrated system needs to be addressed to prevent the leakage of combat information from the Command Post to the integrated systems. In addition to software solutions for data encryption, the solution of using hardware devices to transmit and receive one-way data is a promising avenue for research and investment.

Cite this article : Dung T V, Quyen N T, Nam C H. **Developing a data security solution for the command and control management system at the headquarters**. *Sci. Tech. Dev. J. – Engineering and Technology* 2024, 6(SI8):54-60.

In this article, the application of one-way data transmission devices within the integrated information system equipped at the Military Command Headquarters of the Provincial Military Command [1] will be presented.

RESEARCH METHODS

- Use theoretical analysis and synthesis methods; Analyze actual system requirements.
- Research documents, risks, and security solutions at home and abroad.
- Analyzing and summarizing experience to provide communication solutions to connect the system and security solutions, information security of the system.

INTEGRATED INFORMATION SYSTEM AND HARDWARE SECURITY SOLUTIONS FOR THE SYSTEM

General Introduction to the Operational Management System

The command and control system is located at the Provincial Military Command Headquarters, specifically implemented at the Command Office of the Provincial Military Command and two subordinate units. The system's task is to support command and control activities at various levels of command offices during regular operations as well as in emergency situations. The system allows for the connection of devices placed in different command offices, with the capability to transmit and receive important information that requires high security. In particular, the system enables the connection to existing information systems within the province's territory in cases of defense emergencies, facilitating seamless command and control operations. With this function, the system needs to establish connectivity with the network systems of the establishments to be connected within the province's territory, and the primary task is to ensure the security and protection of information along this connection pathway.

The operational model of the management and operating system is depicted in Figure 1. The significant task of the solution presented in the article aims to propose a hardware solution to ensure the secure protection of information throughout the entire system.

The issue of information protection in the integrated system

To build a system aimed at safeguarding information, it is necessary to consider the following solutions [2]:

- Installing and configuring the database: Organizing a rational network architecture and setting up defense systems help administrators gain an overview of their unit's entire network model. Through this, they can organize a sensible network model and establish essential defense systems such as firewalls, intrusion detection/prevention devices (IDS/IPS).
- Installing protective applications: In addition to troubleshooting system components, this content addresses the installation of protective applications such as antivirus systems and host-based intrusion detection systems (HIDS) to proactively and comprehensively safeguard electronic gateways/websites.

- Establishing backup and recovery mechanisms: Setting up regular backup mechanisms for the system aims to preserve operational states when the system is functioning smoothly. These backup copies will be utilized in the event of system error inspection or system recovery to the state prior to being compromised in cases where the errors are irreparable or cannot be fixed.

Applied to the established system model [1], the author's team proposes the following solution groups [3,4]:

- For the military data transmission network connection, the issues of security, confidentiality, and system safety are under the responsibility of the Cipher committee.
- For the wide area network (WAN) connection of the Command Office, the system is deployed based on the transmission project established by the Provincial Military Command, and the issues of security, confidentiality, and system safety (RCY) constitute a component of this project.
- For the network connection of Committees, Departments, Boards, Sectors, and Police, a one-way data transmission solution is employed for both inbound and outbound directions. The system is designed to ensure grounding, prevent the spread of lightning strikes, and has the capability to isolate the system in case of incidents while restoring the initial state of the Command Office before the installation of equipment.
- In terms of hardware, utilize router firewall devices at the output ports of the system equipment at each Command Office, configuring the packet filtering rules of these devices to allow permitted applications to pass through. Set up blacklist and whitelist configurations to either allow or block specific addresses within the WAN network
- As for software solutions, a group of solutions is employed, including the use of antivirus software utilized

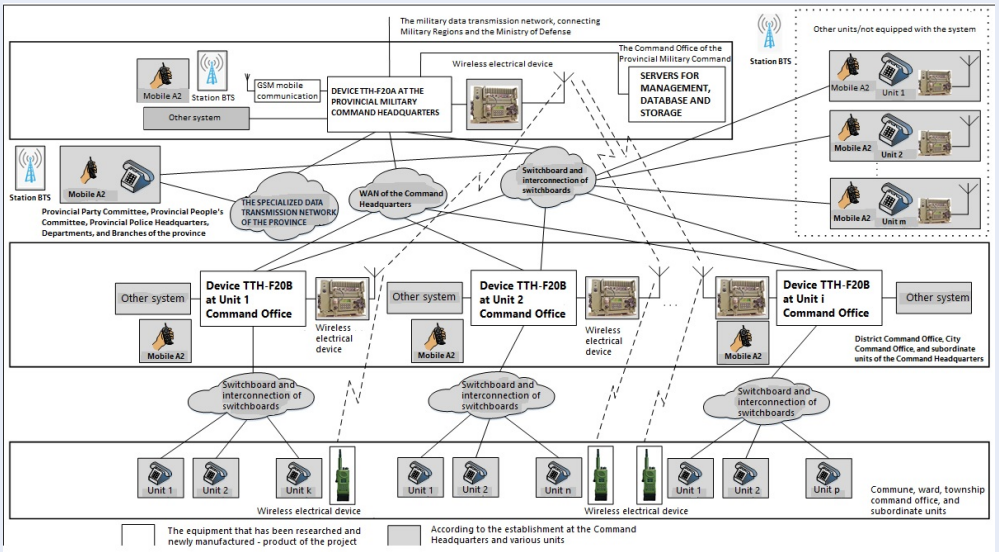

Figure 1: Integrated Two-Level Command and Control Management System

in the military. The authors of the article establish information security regulations within the real-time software execution of virus protection, implement authorization mechanisms for functionalities, and segregate data access permissions within the system to align with the unit's requirements. Access to the system is regulated by granting access privileges according to specific roles, allowing access to critical functions only through corresponding login credentials with appropriate permissions.

- Information stored within the system is encrypted, not stored in plain text, to prevent direct information loss scenarios within the system. Textual and visual information, before being transmitted or received through the system, must pass through the Information Committee to ensure that information is managed by the Information Committee, and then it goes through the Cipher Committee to ensure security as managed by the Cipher Committee. Encryption/decryption can be carried out as required by the information recipient. For critical information such as Command Codes, alarm data, and combat readiness status updates, devices perform encryption/decryption before transmission, utilizing symmetric encryption techniques. The key distribution center is managed by the Provincial Military Command's equipment, and the keys are securely distributed to user units via public-key encryption. There is a mechanism for tracking the usage, access, and exchange of information by user accounts logging into the system.

Hardware solution using one-way data transmission devices

With the system model depicted in Figure 1, it's readily apparent that the network connections within the system can be effectively divided into two distinct subnetworks: the trusted network and the untrusted network. The trusted network serves as the dedicated network for connecting the system components within the Command Office, and between various levels of Command Offices, utilizing the military's private network. The untrusted network encompasses the network systems of local agencies, Provincial Party Committees, and sectors. The primary imperative is to enable the system to establish connections and facilitate data transmission to and from the untrusted network while still ensuring the absolute security of the trusted network. The utmost priority is to prevent any occurrences of data loss or unauthorized data transfer from the trusted network, ensuring no data leakage into the untrusted network.

From the specific requirements mentioned above, it's imperative to introduce protective barriers between the trusted and untrusted networks. There are two approaches in ensuring the system's security[5].

Building on Explicit Policies: This approach involves enforcing safety measures such as unifying the installation of secure applications on the system, coordinating with OS/software providers to request official patches, closing unused ports/services on the system, controlling/monitoring device access, and limiting continuous remote connections.

Proposing a Novel Technological Solution: This approach introduces a security device known as Data Diode. This physical one-way data transmission security device offers a deployment option to ensure quality of service and security [6].

The authors have developed the system with sensitive and critical data that require isolation, yet must also maintain an access authorization policy for authorized users, which can lead to network attack vulnerabilities. The solution the authors have opted for is using the Data Diode security device that only allows one-way information flow, making it impervious to network attacks.

Data Diode devices are most commonly employed in control and automation systems, bank data centers, and military systems. This solution is deployed through two primary models, aimed at preserving the fundamental attributes of a system [5].

Receive – Only – High – Confidentiality Configuration: This configuration maintains the system's security by solely accepting data. In a protected state, the system exclusively receives data from other systems, with no data transmitted in reverse. Potential attacks or exploitation attempts could be directed at the secured network. However, no information from this network can be sent back to the external network.

Transmit – Only – High – Availability Configuration: This configuration ensures the system's availability by only transmitting data. In a safeguarded state, the system solely sends data to other systems and does not accept any incoming data from other systems. Consequently, the protected network cannot be remotely scanned, attacked.

Figure 2 is a diagram that specifically describes how the data diode device works. Accordingly, for OT Network networks, the data diode plays the role of a data control device in the transmit-only direction, and for an IP/CORP network, the data diode device plays the role of a data control device in the receive-only direction.

The choice of hardware security solution depends on the characteristics of each specific system. For military command and control systems, the primary objective is to absolutely prevent any leakage of information from the system. Guided by this criterion, the authors opt for a solution that combines various measures, prominently featuring the utilization of one-way data transmission devices in the communication path to receive data from the trusted network into the untrusted network. The one-way data transmission device is researched with a focus on ensuring secure remote access. Employing this device in the system entails the following advantages and disadvantages:

- Advantages:

+ Ensures security segregation between networks. Network segregation is one of the most effective ways to safeguard networks.

+ Prevents configuration errors that might allow malicious applications to be granted access to the system.

+ Low maintenance costs, as configuring a data diode is straightforward and doesn't require a highly skilled administrator to maintain the system.

+ Data Diode enables real-time data transmission in high-security environments.

- Disadvantages:

+ Data diode equipment can be quite expensive.

+ Using Data Diodes means allowing only one-way communication for certain applications, such as those built on UDP protocol. This necessitates having two data diode devices for transmission and reception, limiting the packet size and reducing transmission speeds.

In summary, comparing the pros and cons above with the system management requirements, Data Diodes emerge as a favorable solution capable of addressing the challenges posed by the authoring team.

1 RESULTS AND DISCUSSION

Figure 3 introduces the network connection and security diagram in the integrated system that the authors implemented at the provincial military command. Through the integrated information system model that has been developed [1], the system can be divided into two components: the internal network and the external network. Accordingly, the internal network represents the network of the provincial military command, while the external network is the specialized data transmission network of the province, connected to the Provincial Party Committee, the Provincial People's Committee, various departments, and the provincial police.

In order to integrate these two network systems to serve the command and control operations, the authors of this study have constructed a model of an integrated network system using one-way data transmission devices known as Data Diodes. The information and data within the internal network will be secured through this solution, in combination with several other measures such as utilizing firewall devices, installing and configuring secure servers, establishing and configuring secure databases, encrypting stored data, encrypting data in transmission, and employing official operating systems/software with patches from manufacturers. Additionally, the security solutions provided by essential agencies will also be incorporated.

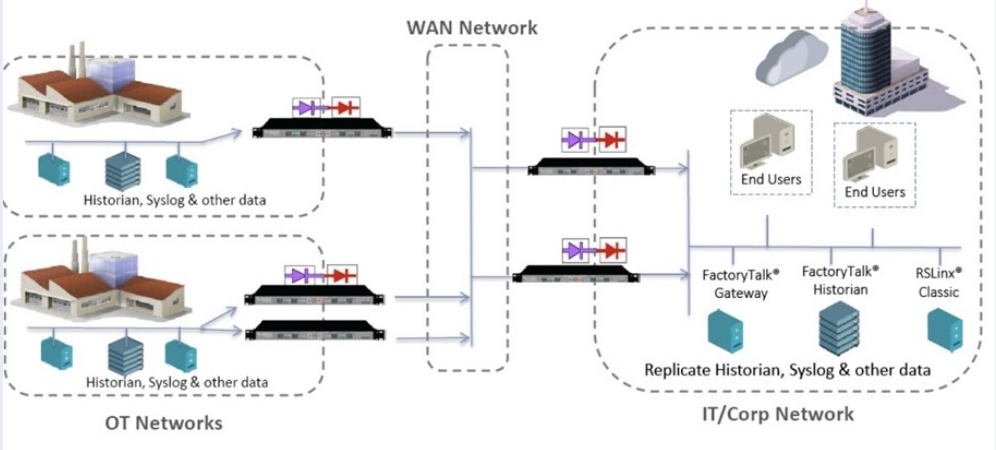

Figure 2: Security system model for data transmission using one-way data transmission device data diode

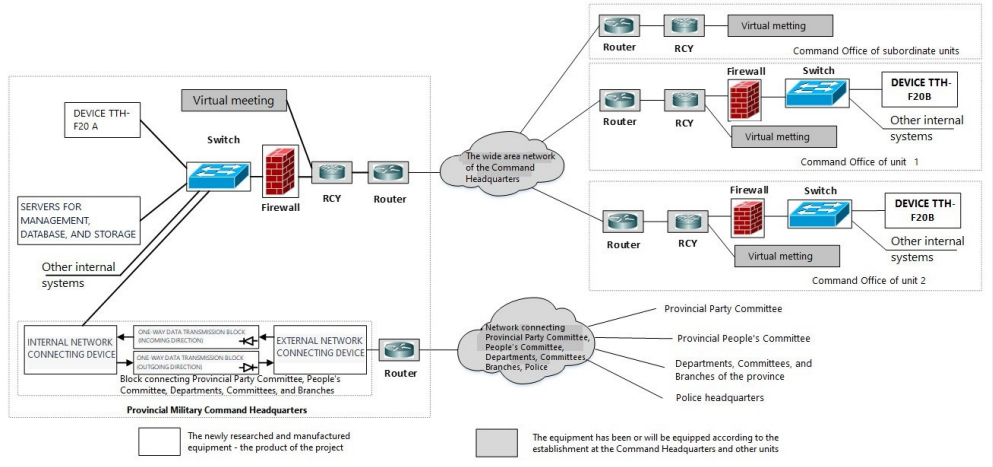

Figure 3: Network connectivity and security diagram in the integrated system at the provincial military command headquarters.

Outcome of building a One-Way data transmission solution for the system with the following parameters:
Functions of the One-Way data transmission device:
- Automatically transmit unidirectional data from the sending side.
- Automatically transmit unidirectional data from the receiving side.
- Monitoring and control function for transmission flow.
- Packet status monitoring function.
- Statistical function for monitoring the number of transmitted and received files.
- Web user interface.
- Allow users to upload and download data files through the web interface.
- Data integrity assurance function.
- All transmitted data is accompanied by a SHA hash value to verify data integrity at the receiving end.
- Personal data security function.
- Each user is provided with a separate login account, and the storage space on the server is completely isolated.
- Supported protocols: UDP, FTP, SFTP, syslog.
- Scalability (Advanced Options):
+ Supported expansion protocols: RTP, Multicast UDP, Modbus, SMB, NTP, SMTP, SMTPS.
+ Expansion features: transmission of various file formats, streaming, database replication.
Table 1 is the technical specifications of the equipment that the authors installed at the provincial mili-

Table 1: Specifications of the Devices

No.	Devices	Configuration
1	Transceiver Unit	- Processing unit: Core i7 10710U upto 4.7GHz, 6 x12, 12MB cache. - Internal memory (RAM): 8GB DDR4 2666MHz. - Hard drive: SSD 256GB.
2	Optoelectronic conversion	- Transmission speed: 10/100/1000 Mbps. - Optical connection standard: SC, 03 fibers. - Internet connection standard: RJ45. - Transmission mode: Single Mode.
3	Connection port	- USB port 3.0: 04. - Ethernet port: 02 (reception and transmission). - HDMI port: 02.

tary command.

CONCLUSION

Based on the previously built information service integration system model [1], the authors used a hardware security solution using a Data Diode one-way data transmission and reception device.

We proposed to create a physically secure one-way channel from the unsecured network to the secure network, allowing data to be securely transferred into the secure network. Not allowing any data to be transferred in the opposite direction ensures that strangers cannot access the secure network from less secure external networks and greatly prevents data leakage.

Once the issue of security and information protection in systems with connections between secure networks and less secure networks is solved, it will promote the ability to integrate systems of domestic units and organizations. That facilitates the formation of a unified integrated system in the future, making information retrieval and search more convenient. This problem not only solves the problem of information transmission and reception between military units and outside units, but also solves the problem of information protection for e-government.

LIST OF ACRONYMS

WAN: Wide area network

CONFLICT OF INTEREST

The authors would like to confirm that there is no conflict of interest in publishing the article.

AUTHOR'S CONTRIBUTIONS

Tran Viet Dung participated in coming up with ideas for writing articles, collecting data and writing the manuscript.

Nguyen Truc Quyen contributed to data interpretation and proofreading the article.

Cu Hoai Nam contributed to the Vietnamese - English translation and edited the article format.

REFERENCES

1. Phuoc HP. A model of an information integration system for handling situations at the Provincial Military Command Headquarters. In: National Workshop on application of high technology into practice - 60 years of development of the Institute of Military Science and Technology; 2020;.
2. Government Cipher Committee - Information Security. Some basic technical measures ensure the safety of portals/websites. 17/11/2012. [Accessed 7 May 2024];Available from: http://antoanthongtin.vn/chinh-sach---chien-luoc/mot-so-bien-phap-ky-thuat-co-ban-dam-bao-an-toan-cho-congtrang-thong-tin-dien-tu-100513.
3. Cyber Information Security Law. Publisher "National Politics"; 2020;.
4. Nguyen AT. Some Basics Of Cyber Security Law. Publisher "People's Public Security"; 2020;.
5. Huyen PT, Anh LD, Government Cipher Committee - Information Security. Data Diode solution for safe one-way data transmission and applications in military countries (Part 1). 18/10/2019. [Accessed 7 May 2024];Available from: https://antoanthongtin.vn/gp-atm/giai-phap-data-diode-truyen-du-lieu-mot-chieu-an-toan-va-ung-dung-trong-quan-doi-cac-nuoc-phan-1-105560.
6. Scott A. Tactical Data Diodes. In: Industrial Automation and Control Systems. SANS Institute; 2015;.

Tạp chí Phát triển Khoa học và Công nghệ – Engineering and Technology 2024, 6(SI8):54-60

Open Access Full Text Article

Bài nghiên cứu

Xây dựng giải pháp bảo mật dữ liệu tác chiến cho hệ thống quản lý điều hành tại sở chỉ huy

Trần Việt Dũng, Nguyễn Trúc Quyên, Cù Hoài Nam*

TÓM TẮT

Bài toán xây dựng hệ thống tích hợp thông tin hỗ trợ công tác chỉ huy điều hành đáp ứng yêu cầu bảo vệ Tổ quốc trong thời chiến cũng như trong thời bình là vô cùng cấp thiết. Và để hệ thống đó có thể áp dụng trong thực tiễn thì cần đảm bảo cả điều kiện cần và điều kiện đủ. Điều kiện cần chính là tính ứng dụng của hệ thống, điều kiện đủ chính là các biện pháp, giải pháp đi kèm của hệ thống nhằm đảm bảo tính toàn vẹn, xác thực của dữ liệu, và đảm bảo dữ liệu không bị rò rỉ thất thoát ra khỏi hệ thống. Hệ thống được triển khai trong môi trường mạng riêng của Sở chỉ huy, đây là lớp mạng cần bảo vệ và không được kết nối internet. Hệ thống mạng được chia ra thành hai phần mạng mật và mạng rõ. Mạng mật chứa dữ liệu của toàn bộ hệ thống, do đó cần kiểm soát tất cả các kết nối đến mạng mật này. Mạng rõ có thể kết nối với các mạng bên ngoài thông qua các thiết bị kiểm soát an toàn thông tin hệ thống. Để đáp ứng các yêu cầu trên hệ thống cần có giải pháp tổng thể về kỹ thuật, về con người. Tuy nhiên trong phạm vi bài báo này, nhóm tác giả trình bày chủ yếu về nhóm các giải pháp phần cứng để giải quyết vấn đề bảo vệ thông tin. Bài viết này xác định các nhóm thông tin cần được bảo vệ, giảm thiểu các mối đe dọa bảo mật và nêu bật các công cụ phần cứng hiện có phù hợp với mô hình hệ thống quản lý vận hành đã thiết lập. Mục tiêu của giải pháp là đảm bảo tính an toàn thông tin tuyệt đối của hệ thống khi triển khai trong các đơn vị quân đội. Bằng các phương pháp thực nghiệm, phân tích và tổng kết lại kinh nghiệm trong quá trình cài đặt và thử nghiệm trong phòng thí nghiệm và thực tế tại đơn vị triển khai chúng tôi đã đạt được hiệu quả đảm bảo được tính an toàn thông tin theo đúng yêu cầu trong quân đội. Tuy nghiên, khi sử dụng giải pháp sẽ làm tăng độ trễ trong việc trao đổi thông tin giữa thiết bị.

Từ khoá: Hệ thống quản lý điều hành, bảo vệ thông tin, giải pháp an toàn phần cứng

Viện Công nghệ thông tin, Thành phố Hồ Chí Minh, Việt Nam

Liên hệ

Cù Hoài Nam, Viện Công nghệ thông tin, Thành phố Hồ Chí Minh, Việt Nam

Email: cuhoainam1234@gmail.com

Lịch sử

- Ngày nhận: 20-9-2023
- Ngày chấp nhận: 27-3-2024
- Ngày đăng: 31-12-2024

DOI : 10.32508/stdjet.v6iSI8.1204

Check for updates

VNUHCM PRESS

Trích dẫn bài báo này: Dũng T V, Quyên N T, Nam C H. **Xây dựng giải pháp bảo mật dữ liệu tác chiến cho hệ thống quản lý điều hành tại sở chỉ huy**. *Sci. Tech. Dev. J. - Eng. Tech.* 2024, 6(SI8):54-60.